UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/222,340	12/28/1998	WILLIAM F. TERRELL	82771.P279	3304

8791 7590 08/21/2009
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
VAUGHN JR, WILLIAM C	

ART UNIT	PAPER NUMBER
2444	

MAIL DATE	DELIVERY MODE
08/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte WILLIAM F. TERRELL and JAMES V. LUCIANI

Appeal 2009-000319
Application 09/222,340[1]
Technology Center 2400

Decided: August 21, 2009

Before JEAN R. HOMERE, ST. JOHN COURTENAY III, and STEPHEN C. SIU, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1 through 14 and 16 through 26. Claim 15 has been cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

[1] Filed on December 28, 1998. The real party in interest is Nortel Networks Limited.

Appellants' Invention

Appellants invented a method and an apparatus for controlling access to a network information source. (Spec. 5, ll. 2-3.) Appellants' Figure 1 depicts a data network (100) comprising a plurality of clients (112, 114, 116, 120, 122, 128, and 130) communicatively coupled to a network core device (108) via network edge devices (110, 118, and 124). (Spec. 8, ll. 7-10.) In particular, network edge devices (110, 118, and 124), in conjunction with a bandwidth broker (126), dynamically create and remove filters that, when triggered, initiate an admission decision controlling provision of an access to the differentiated services of data network (100). (Spec. 8, ll. 14-18.) According to Appellants, the network edge devices (110, 118, and 124) dynamically provision the differentiated services offered by and through a core device (108) on an as-needed and as-authorized bases, thereby minimizing the resources required of the network edge devices (110,118, and 124) and the network (100) to support differentiated services. (Spec. 8, ll. 10-14.)

Illustrative Claim

Independent claim 1 further illustrates the invention as follows:

1. An apparatus adapted to facilitate communications between a client device and a remote device, comprising:

a network interface including (i) filters including at least one filter being triggered to denote when a received packet satisfies filter criteria corresponding to an admission policy related to differentiated service levels, and associated with the at least one filter and (ii) a classifier, communicatively coupled to the filters, to classify and mark one of the service levels associated with the received data packet in response to satisfying the filter criteria associated with the at least one filter; and

a controller coupled to the network interface, to dynamically create and remove the filters controlling access to the different service levels based, at least in part, on an admission profile of the admission policy.

Prior Art Relied Upon

The Examiner relies on the following prior art as evidence of unpatentability:

Lakshman	US 6,341,130 B1	Jan. 22, 2002 (filed Sept. 2, 1998)
Nikander	US 6,253,321 B1	Jun. 26, 2001 (filed Jun. 19, 1998)
Gai	US 6,651,101 B1	Nov. 18, 2003 (filed Jul. 9, 2002)

Barzilai et al., *Design and Implementation of an RSVP-Based Quality of Service Architecture for an Integrated Services Internet* (April 1998), IEEE Journal on Selected Areas of Communications, Vol. 16, No. 3, Pgs. 387-413.

Rejections on Appeal

The Examiner rejects the claims on appeal as follows:

Claims 1 through 11, 13, 14, and 16 through 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lakshman, Barzilai, and Gai.

Claims 12 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lakshman, Barzilai, Gai, and Official Notice.

Appellants' Contentions

1. Appellants contend that the Examiner erred in concluding that the combination of Lakshman, Barzilai, and Gai renders claims 1 through 11, 13, 14, and 16 through 25 unpatentable. In particular, Appellants argue that:

(a) Lakshman's disclosure of filter rules does not teach filter criteria corresponding to an admission policy related to differentiated service levels. (App. Br. 8, Reply Br. 2-3.)

(b) Brazilai's disclosure of a session handle does not teach a classifier to classify and mark one of the differentiated service levels associated with the received data packet. (App. Br. 9, Reply Br. 3.)

(c) Brazilai's disclosure of a QoS Manager that creates, modifies, and removes reservations associated with different flows does not teach a controller to dynamically create and remove the filters controlling access to the different service levels based, at least in part, on an admission profile of the admission policy. (App. Br. 9-10; Reply Br. 3.)

(d) Gai's disclosure of prescribing policy or service treatments to a given traffic flow does not teach dynamically creating and removing filters. (App. Br. 10-11; Reply Br. 3.)

2. Appellants contend that the Examiner erred in concluding that the combination of Lakshman, Barzilai, Gai, and Official Notice renders claims 12 and 26 unpatentable. In particular, Appellants argue that the Examiner's Official Notice stating that it is old and well known for a network administrator to have the capability to remove filters based on an expiration of day or time of data is unsupported by documentary evidence and lacks a clear technical line of reasoning. (App. Br. 11-12.) Further, Nikander's disclosure of an expiration time and data transfer limit relating to a security association does not teach a controller that removes a filter based on time-of-day. (Reply Br. 4.)

Examiner's Findings and Conclusions

1. The Examiner concludes that the combination of Lakshman, Barzilai, and Gai renders claims 1 through 11, 13, 14, and 16 through 25 unpatentable. In particular, the Examiner finds that:

(a) Lakshman's disclosure of filter rules that provide filter criteria used in the processing of received data packets, in conjunction with network service providers that provide different services, teaches filter criteria corresponding to an admission policy related to differentiated service levels. (Ans. 13.)

(b) Barzilai is not relied upon to teach a classifier to classify and mark one of the differentiated service levels. Further, Lakshman's disclosure of a classification processor that receives incoming data packets teaches a classifier to classify and mark one of the differentiated service levels associated with the received data packet. (Ans. 14.)

(c) Brazilai's disclosure of a QoS Manager that creates, modifies, and removes reservations associated with different flows, in conjunction with using dynamically generated filters that provide general and flexible classification of incoming data packets, teaches a controller to dynamically create and remove the filters controlling access to the different service levels based, at least in part, on an admission profile of the admission policy. (Ans. 14-15.)

(d) Gai's disclosure of prescribing policy or service treatments to given data traffic flow teaches dynamically creating and removing filters. (Ans. 15.)

2. The Examiner concludes that the combination of Lakshman, Barzilai, Gai, and Official Notice renders claims 12 and 26 unpatentable. In particular, the Examiner finds that Nikander's disclosure of creating and expiring data packet filters and storing information pertaining to the expiration time and data transfer limit of a security association are both old and well known in the art, and, therefore, teach removing a filter based on time-of-day. (Ans. 15-16.)

II. ISSUES

1. Have Appellants shown that the Examiner erred in concluding that the combination of Lakshman, Barzilai, and Gai renders claims 1

through 11, 13, 14, and 16 through 25 unpatentable? In particular, the issue turns on whether:

(a) Lakshman teaches filter criteria corresponding to an admission policy related to differentiated service levels, as recited in independent claim 1.

(b) Lakshman teaches a classifier, communicatively coupled to the filters, to classify and mark one of the differentiated service levels associated with the received data packet, as recited in independent claim 1.

(c) Barzilai teaches a controller coupled to a network interface, to dynamically create and remove the filters controlling access to the different service levels based, at least in part, on an admission profile of the admission policy, as recited in independent claim 1.

(d) Gai teaches dynamically creating and removing filters, as recited in independent claim 1.

2. Have Appellants shown that the Examiner erred in concluding that the combination of Lakshman, Barzilai, Gai, and Official Notice renders claims 12 and 26 unpatentable? In particular, the issue turns on whether:

(a) Appellants have adequately traversed the Examiner's assertion of Official Notice.

(b) Nikander's disclosure is documentary evidence that is old and well known in the art for a controller to remove a filter based on time-of-day, as recited in dependent claims 12 and 26.

III. FINDINGS OF FACT

The following Findings of Fact ("FF") are shown by a preponderance of evidence.

Lakshman

1. Lakshman generally relates to a data packet filter associating at least one filter rule with a data packet, each filter rule and the data packet are characterized by values in first and second dimensions. The filter rule is applied to the data packet by a router in a communications network. (Col. 3, ll. 53-57.)

2. Lakshman discloses that network service providers, while using a shared backbone infrastructure, may provide different services to different customers based on different requirements. (Col. 1, ll. 54-56.) Such requirements may be different service pricing, security, or Quality of Service ("QoS"). (Col. 1, ll. 56-58.) To provide these differentiated services, routers typically include a mechanism for 1) classifying and isolating traffic, or data packet flows, from different customers, 2) preventing unauthorized users from accessing specific parts of the network, and 3) providing customized performance and bandwidth in accordance with customer expectations and pricing. (Col. 1, ll. 58-64.)

3. Lakshman's Figure 2 depicts a router (245) of a network node receiving streams or flows of data packets from input links (247) and routing these data packet streams or flows to output links (260). (Col. 1, ll. 35-37.)

To perform a forwarding function, a router (245) receives a data packet at an input link (247). Further, a control mechanism (250) within the router utilizes an independent generated look-up table to determine which output link (260) the data packet should be routed to. (Col. 1, ll. 37-42.) In addition to the data packet forwarding function, the router (245) may perform a data packet filtering function. (Col. 1, ll. 65-67.) To perform data packet filtering, the router (245) may be provided with a table or a list of filter rules specifying that routing of data packets sent from one or more specified sources is denied or that a specific action is taken for a data packet having a specified source address. (Col. 2, ll. 3-7.) Thus, a variety of filter rules may be implemented based on data packet field information. (Col. 2, ll. 20-22.) For example, such filter rules might be based on 1) source address; 2) destination address; 3) source ports; 4) destination ports; and/or 5) any combination of these fields. (Col. 2, ll. 22-24.) Filter rules are applied to every data packet that the router receives; that is, for each data packet received by the router, every filter rule is successively applied to each data packet to ascertain whether that data packet is to be forwarded, restricted, or re-routed according to the filter rule. (Col. 2, ll. 31-35.)

4. Lakshman discloses that data packet filtering parses fields from the data packet header including, for example both the source and destination address. (Col. 2, ll. 9-11.) Parsing allows each incoming data packet to be classified using filter rules defined by network management software, routing protocols, or real-time reservation protocols such as

Reservation Set-up Protocol ("RSVP"). (Col. 2, ll. 11-14.) Packet classification processes the received data packets using the field or other parameter information in the data packet. (Col. 6, ll. 17-19.) In particular, Lakshman's Figure 11 depicts a classification processor (1050) that receives the incoming data packet and stores field parameters, e.g., source address and destination address S and D, in a register (1176). (Col. 14, ll. 12-15.)

Barzilai

5. Barzilai discloses resource management protocol stack extensions, and device support required at the end hosts to enable an end-to-end RSVP QoS infrastructure in the Internet. (Pg. 397, col. 2, ll. 20-23.) In particular, Barzilai concentrates on the design and implementation of QoS support on Unix variant Internet servers. (Pg. 397, col. 2, l. 23-25.) One of the primary goals in designing the service architecture is to blend the QoS support with the existing Internet Protocol Suite ("TCP/IP") stack and socket Application Program Interface ("API"), such that the structure of the Unix networking subsystem is preserved. (Pg. 397, col. 2, ll. 26-29.)

6. Barzilai discloses that the heart of the resource management and control architecture is the QoS Manager. (Pg. 398, col. 2, ll. 44-45.) From the functional point of view, it is a control plane component primarily responsible for the creation, modification, and removal of reservations associated with different flows or data packets. (Pg. 398, col. 2, ll. 45-48.)

7. Barzilai discloses that data packet filters provide general and flexible classification of incoming data packets to application endpoints. (Pg. 411, col. 2, ll. 19-21.) More recently, dynamic code generation techniques have been applied to realize very efficient data packet filters. (Pg. 411, col. 2, ll. 21-23.)

Nikander

8. Nikander generally relates to a system that implements a security protocol based on processing data packets. (Abstract.) The data processing system comprises processing data packets for storing filter code and processing data packets according to stored filter code, and a policy managing function for generating filter code and for communicating generated filter code for data packet processing. (Abstract.)

9. A device or process responsible for implementing the data packet transformations according to the IP security protocol ("IPSEC") method in a network device is generally called an "IPSEC engine." (Col. 4, ll. 24-27.) The IPSEC engine must deal with security association creation and expiration and consult external key managers. (Col. 4, ll. 38-40.) Security association parameters are information needed to apply an IPSEC transformation to a data packet. (Col. 6, ll. 62-64.) Nikander's Figure 4 depicts the main data items to be stored in a security association. (Col. 7, ll. 4-5.) Cell 406 includes the expiration time and data transfer limit of the security association. (Col. 7, ll. 11-13.)

IV. PRINCIPLES OF LAW

Obviousness

"On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness." *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998).

> Section 103 forbids issuance of a patent when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains."

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 406 (2007).

In *KSR*, the Supreme Court emphasized "the need for caution in granting a patent based on the combination of elements found in the prior art," and discussed circumstances in which a patent might be determined to be obvious. *Id.* at 415 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 12 (1966)). The Court reaffirmed principles based on its precedent that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* at 416. The operative question in this "functional approach" is thus "whether the improvement is more than the predictable use of prior art elements according to their established functions." *Id.* at 417.

In identifying a reason that would have prompted a person of ordinary skill in the relevant field to combine the prior art teachings, the Examiner must show some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *KSR,* 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

Official Notice

The Examiner may take notice of facts or common knowledge in the art which are capable of such instant and unquestionable demonstration as to defy dispute. *In re Ahlert*, 424 F.2d 1088, 1091 (CCPA 1970). To challenge the Examiner's notice, Appellants must present evidence to the contrary. *In re Knapp-Monarch Co*. 296 F.2d 230, 232 (CCPA 1961) (considering challenge to taking of judicial notice by Trademark Trial and Appeal Board).

V. ANALYSIS

Claim 1

Independent claim 1 recites, in relevant parts:

> [1)] at least one filter being triggered to denote when a received packet satisfies filter criteria corresponding to an admission policy related to differentiated service levels; [2)] a classifier, communicatively coupled to the filters, to classify and mark one of the service levels associated with the received data packet in response to satisfying the filter criteria associated with the at least one filter; and [3)] a controller coupled to the network interface, to dynamically

> create and remove the filters controlling access to the different service levels based, at least in part, on an admission profile of the admission policy.

As set forth in the Findings of Fact section above, Lakshman discloses associating at least one filter rule with a data packet whereby the filter rule is applied to the data packet by a router coupled to a control mechanism. (FF 1, 3.) In particular, Lakshman discloses implementing a variety of filter rules to each data packet. (FF 3.) Filter rules are successively applied to every data packet that the router receives in order to ascertain whether the data packet should be forwarded, restricted, or re-routed. (*Id.*) We find that Lakshman's disclosure teaches a router coupled to a control mechanism that applies filter rules to a data packet and forwards, restricts, or re-routes the data packet accordingly. Further, Lakshman discloses that network service providers provide different services to different customers based on different requirements. (FF 2.) We find that Lakshman's disclosure of network service providers that provide different services teaches differentiated service levels. In summary, we find that Lakshman's disclosure of a router coupled to a control mechanism that applies filter rules to a data packet and forwards, restricts, or re-routes the data packet accordingly, in conjunction with differentiated service levels, teaches at least one filter being triggered to denote when a received packet satisfies filter criteria corresponding to an admission policy related to differentiated service levels, as recited in independent claim 1.

Further, as set forth in the Findings of Fact section above, Lakshman discloses that an incoming data packet is classified using filter rules defined by network management software. (FF 4.) In particular, Lakshman's discloses a classification processor that receives the incoming data packet and stores field parameters for classification processing. (*Id.*) We find that Lakshman's disclosure teaches classifying a data packet according to filter rules defined by software. As set forth above, we find that Lakshman's disclosure teaches differentiated service levels. In summary, we find that Lakshman's disclosure of classifying a data packet according to filter rules defined by software, in conjunction with differentiated service levels, teaches a classifier, communicatively coupled to the filters, to classify and mark one of the service levels associated with the received data packet in response to satisfying the filter criteria associated with the at least one filter, as recited in independent claim 1.

Additionally, as set forth in the Findings of Fact section above, Barzilai discloses both the design and implementation of QoS support on various Internet servers. (FF 5.) In particular, Barzilai discloses that the QoS Manager is a component primarily responsible for the creation, modification, and removal of reservations associated with different data packets. (FF 6.) Further, Barzilai discloses that data packet filters provide general and flexible classification for incoming data packets and apply dynamic code generation techniques to create more efficient data packet filters. (FF 7.) We find that Barzilai's disclosure of a QoS Manager teaches a controller that applies dynamic techniques to data packet filters in order to create, modify, and remove data packets. As set forth above, we find that Lakshman's disclosure teaches differentiated service levels. In summary, we find that Barzilai's disclosure of a controller that applies dynamic techniques to data packet filters in order to create, modify, and remove data packets, in conjunction with Lakshman's disclosure of differentiated service levels, teaches a controller to dynamically create and remove the filters controlling access to the different service levels based, at least in part, on an admission profile of the admission policy, as recited in independent claim 1. Thus, it follows that the Appellants have not shown that the Examiner erred in concluding that the combination of Lakshman and Barzilai renders independent claim 1 unpatentable.

Since Appellants have not shown that the Examiner erred in concluding that the combination of Lakshman and Barzilai renders independent claim 1 unpatentable, it follows that Appellants have also not shown that the Examiner erred in concluding that the combination of Lakshman, Barzilai, and Gai renders independent claim 1 unpatentable.

Appellants do not provide separate arguments with respect to claims 2 through 11, 13, 14, and 16 through 25. Therefore, we select claim 1 as being representative of the cited claims. Consequently, claims 2 through 11, 13, 14, and 16 through 25 stand or fall with representative claim 1. 37 C.F.R. § 41.37(c)(1)(vii).

Claims 12 and 26

Dependent claims 12 and 26 recite, in relevant part, wherein the controller [means] removes at least one of the filters based, at least in part, on time-of-day.

MPEP § 2144.03(C) provides the requirements to traverse Official Notice: "[S]pecifically point out the supposed errors in the [E]xaminer's action, which would include stating why the noticed fact is not considered to be common knowledge or well-known in the art." *See* 37 C.F.R. 1.111(b). *See also In re Chevenard*, 139 F.2d 711, 713 (CCPA 1943). Appellants have failed to adequately traverse the Official Notice because Appellants have only made a general allegation that the notice was not proper without actually addressing why any of the facts would not be common knowledge. Nonetheless, the Examiner provides documentary evidence in the Examiner's Answer. As set forth in the Findings of Fact section above, Nikander discloses a data processing system that processes data packets according to filter code. (FF 8.) In particular, Nikander discloses an engine that deals with information needed to apply added security to a data packet, including the expiration time and data transfer limit. (FF 9.) We find that Nikander's disclosure teaches filtering data packets whereby an engine utilizes the creation time and expiration time of each data packet. In particular, we find that Nikander's disclosure of filtering data packets whereby an engine utilizes the creation time and expiration time of each data packet amounts to filtering information based on time-of-day. As set forth above, we find that Barzilai's disclosure teaches a controller that applies dynamic techniques to data packet filters in order to create, modify, and remove data packets. In summary, we find that Nikander's disclosure of filtering data packets whereby an engine utilizes the creation time and expiration time of each data packet, in conjunction with Barzilai's disclosure of a controller that applies dynamic techniques to data packet filters in order to create, modify, and remove data packets, teaches a controller that removes at least one of the filters based on time-of-day. We are satisfied that the Examiner has provided sufficient documentary evidence to maintain the Examiner's assertion of Official Notice. It follows that the Appellants have not shown that the Examiner erred in concluding that the combination of Lakshman, Barzilai, Gai, and Official Notice renders dependent claims 12 and 26 unpatentable.

VI. CONCLUSIONS OF LAW

Appellants have not shown that the Examiner erred in concluding that:

1. the combination of Lakshman, Barzilai, and Gai renders claims 1 through 11, 13, 14, and 16 through 25 unpatentable under 35 U.S.C. § 103(a).

2. the combination of Lakshman, Barzilai, Gai, and Official Notice renders claims 12 and 26 unpatentable under 35 U.S.C. § 103(a).

VII. DECISION

We affirm the Examiner's decision to reject claims 1 through 14 and 16 through 26 under 35 U.S.C. § 103(a).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

rwk

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040